



Interview Questions on **Cyber Attacks**

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

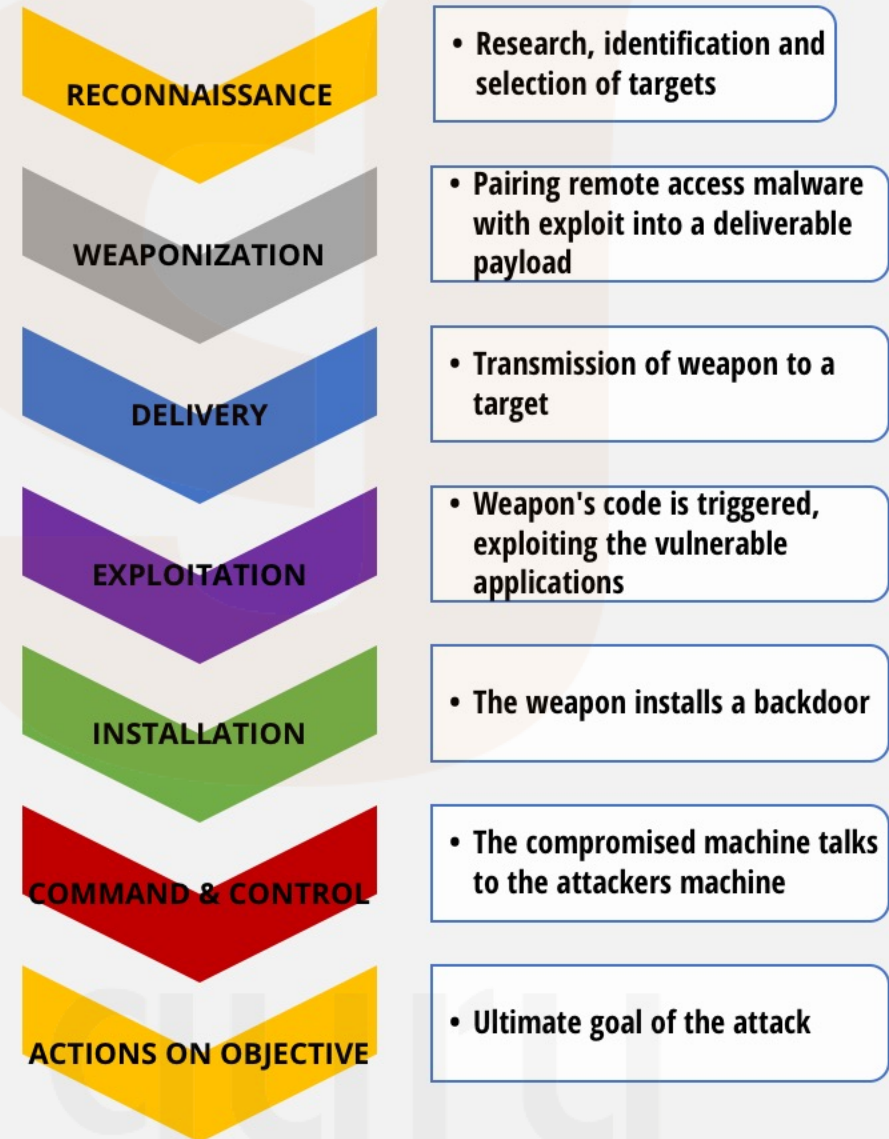
<https://socexperts.com>

What is Cyber Kill Chain?

Cyber Kill Chain defines the steps used by an attacker to launch and carry-out a cyber attack.

It is defined by **Lockheed Martin**

It has **7 phases**



What is MITRE ATT&CK Framework?

- The **MITRE** ATT&CK framework is a comprehensive matrix of **tactics** and **techniques** used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk.
- It highlights 12 Tactics and more than 250 Techniques that attackers use

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe

What are TTPs?

TTPs stand for Tactics, Techniques and Procedures

TTPs are patterns of activities or methods associated with a specific threat actor or group of threat actors.

What is Zeroday?

A vulnerability or a malware that has been identified but doesn't have a fix (patch or signature) yet.

It is the time period between a vulnerability/malware being identified and release of patch/signature.

What is an exploit and payload?

Exploit is a tool that takes advantage of a vulnerability. Usually exploit is used to penetrate into a system taking advantage of an existing vulnerability.

Example – EternalBlue that took advantage of SMB vulnerability

Payload is the actual malware. Part of the malware that does the damage (deleting files, stopping services, encrypting files, gathering and sending sensitive information, taking pictures etc.)

Example – WannaCry used EternalBlue as exploit and had the ultimate intention of encrypting the files and demand ransom.

Explain Brute-force attack.

Brute-force is a password guessing attack. It tries various combinations of usernames and passwords again and again until it gets in.

Mitigation:

- Encourage users to use complex passwords
- Lockout accounts after few attempts
- Use Captcha to slow down brute-force
- Use multifactor authentication

Explain Dictionary attack.

Dictionary attack is type of brute-force attack. It uses a list of words in a dictionary as passwords.

Dictionary attack can also be personalized by using details of the target like date of birth, spouse name, children name, vehicle number etc.

Mitigation:

- Advise users not to keep a simple word or easily identifiable information as password.
- Encourage users to use complex passwords
- Lockout accounts after few attempts
- Use Captcha to slow down brute-force
- Use multifactor authentication

Explain Rainbow attack.

Rainbow attack is a type of brute-force attack that uses pre-computed password hashes. i.e. instead of trying to pass the password, it tries to match the hash in the user database.

Mitigation:

- Rainbow table attacks can easily be prevented by using salt techniques,
 - **Salt** is a random data that is passed into the hash function along with the plain text.
- Lockout accounts after few attempts
- Use Captcha to slow down brute-force
- Use multifactor authentication

What is Pass-the-hash attack

Pass the hash is a hacking technique that allows an attacker to authenticate to a remote server or service by using the underlying hash of a user's password, instead of requiring the associated plaintext password as is normally the case.

This will reduce the effort of the attacker as he does not have to crack the plaintext password from the stolen hash.

Mitigation:

- Restrict and protect high privileged domain accounts
 - This mitigation reduces the risk of administrators from inadvertently exposing privileged credentials to higher risk computers.
- Restrict and protect local accounts with administrative privileges
 - This mitigation restricts the ability of attackers to use administrative local accounts for lateral movement Pth attacks.
- Restrict inbound traffic using the Windows Firewall
 - This mitigation restricts attackers initiating lateral movement from a compromised workstation by blocking inbound connections on all other workstations with the local Windows Firewall.

What is Scanning?

Scanning is a method for discovering exploitable communication channels.

Scanning for open ports

Scanning for known vulnerabilities

Mitigation:

- Use Firewall and IPS
- OS Hardening
- Use honeypots to detect scanning activities

What is Sniffing Attack?

Sniffing corresponds to theft or interception of data by capturing the network traffic when it flows through a computer network.

Usually done using a packet sniffer

Mitigation:

- Avoid using insecure protocols (like HTTP, FTP, telnet etc. and use secured versions like HTTPS, SFTP, SSH etc.)
- Use encryption whenever possible for data transmission.

What is Spoofing?

Spoofing is a malicious practice employed by cyber scammers and hackers to deceive systems, individuals, and organizations into perceiving something to be what it is not.

Few types of Spoofing

- IP Spoofing
- MAC Address Spoofing
- Email Spoofing
- DNS Spoofing

Mitigation:

- Deploy IPS (IP Spoofing)
- Educate users (Email Spoofing)
- Enable port level security (ARP and MAC Address Spoofing)

Explain Phishing.

- Phishing is a cyber attack that uses disguised email as a weapon.
- The goal is to trick the email recipient into believing that the message is something they want or need
- Example: a request from their bank, for instance, or a note from someone in their company
- Ultimate intention is to get the user to click a link or download an attachment.

Mitigation:

- Use Email Security Solutions (to block obvious phishing and spam emails)
- Educate users
- Use DMARC (Domain-based Message Authentication, Reporting and Conformance)
 - DMARC is a standard for verifying the authenticity of an email. It offers email receivers a way to verify if a message is really from a authorized sender or not.

Other Phishing Attacks

Explain Spear Phishing.

Spear phishing is an email scam targeted towards a **specific** individual, organization or business.

Attackers use the information they have gathered during reconnaissance to make the email appear personalized.

Explain Whaling.

Whaling is a type of phishing that targets senior management/leadership teams/important individuals at an organization

Explain Vishing.

Vishing works similar to phishing, instead of sending an email, the attacker tricks the target to give critical/sensitive information over a phone call

Explain DOS and DDOS attack.

Denial-of-Service (DOS) is a type of cyberattack in which the attacker seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services.

Examples:

UDP floods, ICMP floods, SYN floods, fragmented packet attacks, Ping of Death etc.

Distributed Denial-of-Service (DDOS) is a type of attack where multiple systems are used to launch DOS attack on one targeted system.

Usually DDOS are result of multiple compromised systems (called Botnets)

Mitigation:

- Use Anti-DDOS technology (like Arbor)
- Rate limit (limit the number of connections from an IP or User)
- Reduce connection wait time
- Deploy load balancers

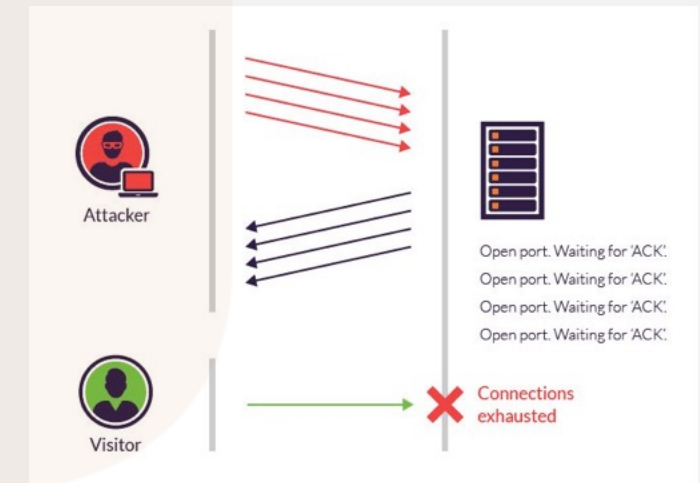
Explain SYN flood attack.

SYN Flood attack is a type of DOS attack where it exploits the normal TCP three-way handshake.

The attacker send huge connection requests (SYN) but never sends an acknowledge back to the sever. This will make the server wait for certain time and hold the connection. This will consume all the concurrent connections on the target server making it inaccessible for legit users.

Mitigation:

- Use Anti-DDOS technology (like Arbor)
- Rate limit (limit the number of connections from an IP or User)
- Reduce connection wait time
- Deploy load balancers



Explain ARP poisoning.

- Also called as ARP Spoofing
- ARP poisoning is when an attacker sends falsified ARP messages over a local area network (LAN) to link an attacker's MAC address with the IP address of a legitimate computer or server on the network.
- It is used to do a Man-in-the-Middle attack

Mitigation:

- Use Static ARP
- Detect ARP poisoning using tools like XARP
- Set up Packet filtering
- Install AV and keep signatures updated

Explain MITM attack.

Man-in-the-Middle is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

Mitigation:

- Use Static ARP (to prevent ARP poisoning)
- Use Encryption (prevent the attacker from leveraging the data)
- IPS system (can detect sudden change in the network performance)

Explain DNS Poisoning.

- Also called as DNS Spoofing
- Type of cyberattack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones.
- This is done by introducing corrupt (poisoned) DNS data into DNS Resolver's Cache.

Mitigation:

- Regularly audit DNS Zones
- Keeping DNS Servers up-to-date.
- Restrict Zone Transfers
- Limit recursive queries.
- Store only data related to the requested domain.

What is DNS Tunneling?

- DNS Tunneling is a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses.
- Usually DNS traffic is allowed through firewalls and attackers take advantage of this.
- It is used for data exfiltration (without being detected)

Mitigation:

- IPS Systems can help detect few DNS Tunneling attacks
- Block communication to IPs that are known to be used for data exfiltration
- Use DNS firewall
- Deploy standalone DNS protection solution (Like Infoblox)

What is a malware?

- Malware is a (malicious) software intentionally designed to cause damage to a computer or computer network.
- The malicious activities include
 - Deleting files
 - Encrypting files
 - Gain access of the infected machine
 - Collecting and sending sensitive data
 - Stopping services
 - System shutdown etc.

Mitigation:

- Use AV with up-to-date signature
- Use Ad-blockers
- Educate users not to download files from unknown sources

Explain different Types of Malware.

Virus: Viruses attach themselves to clean files and infect other clean files. Their intention is to damage a system's core functionality and deleting or corrupting files. They usually appear as an executable file (.exe).

Trojans: This kind of malware disguises itself as legitimate software but has malicious intent. It tends to act discreetly and create backdoors in your security to let other malware in.

Worms: Worms infect entire networks of devices, either local or across the internet, by using network interfaces. It uses each consecutively infected machine to infect others.

Spyware: Spyware is malware designed to spy on you. It hides in the background and takes notes on what you do online, including your passwords, credit card numbers, surfing habits, and more.

Ransomware: This kind of malware typically locks down your computer and your files, and threatens to erase everything unless you pay a ransom.

Adware: Though not always malicious in nature, aggressive advertising software can undermine your security just to serve you ads — which can give other malware an easy way in. Plus, they end up consuming system resources

Botnets: Botnets are networks of infected computers that are made to work together under the control of an attacker.

RAT: Remote Access Trojan – Type of malware that allows an attacker gain unauthorized remote access of victim's machine

Difference between Virus and Trojan and Worm?

Virus: Viruses attach themselves to clean files and infect other clean files. A user action (like execution) is required for the virus to run.

Trojans: They appear as useful programs, but have malicious intentions. Trojans are usually used to trick the user into performing certain action (like execution)

Worms: Worm spread in the network without user actions. They spread by

- Attached external storage
- Available open network shares
- Email (a worm can automatically send a copy of itself to all the users in your address book)

What is drive-by-download?

- A drive-by download refers to the unintentional download of malicious code onto a computer or mobile device that exposes users to different types of threats.
- In this type of attack, users need not click on anything to initiate the download. Simply accessing or browsing a website can activate the download.
- Drive-by download happens by taking advantage of insecure, vulnerable, or outdated apps, browsers, or even operating systems.

Mitigation:

- Encourage users to keep their software up to date
- Install AV that is capable of scanning internet traffic
- Install web-filtering software.
- Restrict add-ons on browsers.
- Educate users not to visit untrusted websites.

What is fileless malwares or fileless attack?

- Fileless malware sneaks in without using traditional executable files as a first level of attack.
- Rather than using malicious software or downloads of executable files as its primary entry point onto corporate networks, fileless malware often hides in memory or other difficult-to-detect locations.
- Uses living-off-the-land techniques
- Fileless malware leverages trusted, legitimate processes running on the operating system to perform malicious activities.
- Simply put, fileless malware run on RAM (memory-based) and doesn't have any trace on the Disk (file-based). This makes it impossible for a traditional antivirus which rely on signatures to detect a malware.

Mitigation:

- Use EDR tools to monitor and detect suspicious activities.
- Disable command line shell scripting language, including PowerShell and Window Management instrumentation, wherever it's not needed

What is OWASP?

The Open Web Application Security Project (OWASP) is an online community that produces articles, methodologies, documentation, tools, and technologies in the field of web application security.

Every year OWASP announces List of Top 10 Vulnerabilities for Web Applications – OWASP Top 10

As of 2019, top 10 web application attack/vulnerabilities are:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XEE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting
- Insecure Deserialization
- Using Components With Known Vulnerabilities
- Insufficient Logging And Monitoring

Explain SQL Injection.

SQL injection is a code injection technique in which malicious SQL statements are inserted into an entry field for execution.

These SQL statements control a database server behind a web application. By executing malicious statements, the attacker can gain unauthorized access, copy, modify or delete the data.

Example of malicious SQL Statement: ' OR '1'='1' --

Mitigation:

- Input validation
- Sanitize all inputs (like remove quotes and special characters)
- Use IPS and WAF solutions
- Turn off visibility of Database errors on production servers

Explain Cross Site Scripting (XSS).

Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.

Usually happens where there is a text message box in the website. Like comments for a blog.

Mitigation:

- Input validation
- Sanitize all inputs (like remove quotes and special characters)
- Encode data on output.

Explain Cross Site Request Forgery (CSRF).

- Also called as **one-click attack** or **session riding**
- Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

Example:

- User A is connected to a banking website – www.mybank.com
- Attacker tricks the user into downloading and executing a code.
- This code will send request to www.mybank.com to transfer money to attackers account.
- In this case the banking website performs the request because it see the request coming from User A's machine who is already authenticated with the server.

Mitigation:

- Synchronizer token pattern
- Cookie-to-header token
- Double Submit Cookie

Explain Broken Authentication.

Broken Authentication weaknesses can allow an attacker to either capture or bypass the authentication methods that are used by a web application.

- Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.
- Permits brute force or other automated attacks.
- Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin".
- Uses weak or ineffective credential recovery and forgot-password processes.
- Uses plain text or weakly hashed passwords

Mitigation:

- Where possible, implement multi-factor authentication to prevent automated, credential stuffing, brute force, and stolen credential re-use attacks.
- Do not ship or deploy with any default credentials, particularly for admin users.
- Implement weak-password checks, such as testing new or changed passwords against a list of the top 10000 worst passwords.
- Lock user accounts after certain failed attempts

Explain Broken Access Control.

Broken Access Control is a weakness in web application that will let the users do more than what they are authorized. Example, user A can see the details of user B.

Broken Access Control vulnerabilities often lead to

- unauthorized information disclosure
- modification or destruction of all data
- performing a business function outside of the limits of the user.

Mitigation:

- Deny access to functionality by default.
- Use Access control lists and role-based authentication mechanisms.
- Log access control failures, alert admins when appropriate (e.g. repeated failures).